**26. Ortstagung Bremen am 14. März 2011**

Für die 26. Ortstagung des Arbeitsgerichtsverbandes in Bremen am 14. März 2011 konnte als Gast *Prof. Dr. Peter Wedde* von der Fachhochschule Frankfurt am Main gewonnen werden. *Wedde* ist als Professor für Arbeitsrecht und Recht der Informationsgesellschaft tätig. Er referierte über das Thema „Der gläserne Arbeitnehmer".

Zunächst begrüßte die Präsidentin des Landesarbeitsgerichts Bremen *Sabine Kallmann* in der gastgebenden Arbeitnehmerkammer die zahlreichen Zuhörer und stellte den Referenten vor. Danach übergab sie an *Michael Grauvogel*, Vizepräsident des Landesarbeitsgerichts Bremen, die Moderation.

*Wedde* stellte vorab die aktuelle Lage hinsichtlich der Schaffung eines Beschäftigtendatenschutzgesetzes dar. Die Datenschutzskandale in den letzten Jahren im arbeitsrechtlichen Bereich seien dabei Ausgangspunkt für die neue Diskussion über ein einheitliches Beschäftigungsdatenschutzgesetz gewesen.

In einem ersten Teil stellte *Wedde* zur Einführung Praxisbeispiele vor, leitete dann zu den technischen Einrichtungsmöglichkeiten zur Überwachung von Beschäftigten über und bewertete in einem letzten Schritt die Situation aus arbeitsrechtlicher und datenschutzrechtlicher Sicht.

## 1. Einführung in das Thema anhand von Praxisbeispielen

Neben den durch die Medien allseits bekannten Vorfällen machte *Wedde* zunächst auf einen Fall aufmerksam, der sich so in einer bundesdeutschen Landesverwaltung zugetragen haben soll. Dort erteilte der Arbeitgeber die Anweisung, dass alle Beschäftigten im Falle ihrer Abwesenheit einen Umleitungsassistenten einschalten sollen, der alle E-Mails an einen vom Arbeitgeber benannten Vertreter weiterleitet. Begründet wurde dieses Verlangen damit, dass es keine Geheimnisse mehr gebe, da aufgrund des Verbots der privaten Nutzung alle E-Mails dienstlicher Natur seien.

In einem zweiten Beispielsfall seien in einer Vertriebsorganisation Mobiltelefone mit einer Android-Software („Google-Handys") eingeführt worden, die entsprechend den Bedürfnissen des Arbeitgebers diesem Informationen darüber übermittelten, wo sich der Arbeitnehmer befindet, was für Termine er wahrnimmt und welche Telefongespräche er geführt hat. Die betroffenen Arbeitnehmer hatten hiervon keine Kenntnis.

Einen dritten Vorfall aus der Praxis schilderte *Wedde* wie folgt: Ein Arbeitnehmer ist aufgrund eines Unfalls für längere Zeit arbeitsunfähig erkrankt. Da der Arbeitgeber in dieser Situation die sich auf dem PC des Arbeitnehmers befindenden Daten benötigt, lässt er das Passwort „knacken" und findet in der Folge neben den dienstlichen Daten eine umfassende Sammlung von mp3-Musikfiles sowie zahlreiche Videokopien aktueller Spielfilme. Da die private Nutzung des Computers bei dem Arbeitgeber verboten ist, mahnt er den Arbeitnehmer ab. Nachdem sich der Arbeitnehmer gegen die Abmahnung zur Wehr setzt, nimmt der Arbeitgeber die Abmahnung zurück.

In einem weiteren Fall berichtete *Wedde* von einem Unternehmen, in dem auf der Grundlage von Vertrauensarbeitszeit gearbeitet wird. Der Arbeitgeber wolle mit der Begründung, dass es sich nur so verhindern lasse, dass Beschäftigte ihre Arbeitszeit damit verschwendeten, private E-Mails zu schreiben, alle E-Mails kontrollieren. Als er auf entsprechenden Widerstand stößt, nimmt er das Ansinnen zurück.

Ein weiterer kurioser Fall soll sich so in der deutschen Niederlassung eines US-amerikanischen IT-Konzerns abgespielt haben. Alle Innenräume und die Gebäude im Außenbereich werden dort durch Videokameras überwacht. Die Beobachtung der Monitore erfolgte lange Zeit direkt vor Ort durch den Wachdienst. Ohne Kenntnis des Betriebsrats verlagerte der Arbeitgeber die Überwachung der Monitore aus Kostengründen nach Italien. Er war der Auffassung, ein Mitbestimmungsrecht bestehe nicht. Eines Nachts konnte der Sicherheitsdienst in Italien beobachten, wie in eine bayerische Niederlassung eingebrochen wurde und rief umgehend bei der Polizei in Bayern an. Diese konnte den Sicherheitsdienst aus Italien nicht verstehen. Durch den Einbruch entstand ein immenser Schaden. In der Zwischenzeit wurde die Überwachung der Monitore wieder nach Deutschland verlegt.

Ferner machte *Wedde* darauf aufmerksam, dass sowohl bei der Daimler AG als auch beim NDR im Rahmen von Einstellungsverfahren von den Bewerbern die Abgabe von Blut- und Urintests gefordert wurde. Zwischenzeitlich wurde diese Praxis wieder eingestellt.

In einem letzten Beispielsfall schilderte *Wedde* die grenzenlose Kundendienstfreundlichkeit eines deutschen Unternehmens, welches zu einem großen europäischen Konzern gehört. Dieses Unternehmen teilte seinem Betriebsrat vor einiger Zeit mit, dass es beabsichtige, die Daten ihrer Beschäftigten in die USA zu übermitteln bzw. einen Zugriff der Sicherheitsbehörden auf die entsprechenden Datenbanken freizugeben. Das Unternehmen begründete diesen Schritt damit, dass dies im Rahmen eines Angebots für einen sehr großen Auftrag mit Sicherheitsrelevanz verlangt werde. Einen Handlungsspielraum hatte das Unternehmen nach eigenen Angaben nicht.

Im Ergebnis hielt *Wedde* fest, dass sich die Anzahl an Beispielfällen weiter fortsetzen lasse und er davon ausgehe, dass die Zahl der Fälle in Zukunft deutlich zunehmen werde. Einer der Gründe hierfür sei die Vielzahl neuer technischer Möglichkeiten, die den Arbeitgebern zur Verfügung stünden, womit *Wedde* zu seinem zweiten Teil des Vortrags kam.

## 2. Überlegungen zu technischen Einflussfaktoren

In diesem Teil seines Vortrags erläuterte *Wedde* die Problematik des technischen Fortschritts im Hinblick auf die Möglichkeiten, die Arbeitgebern geboten würden, um Daten und Informationen über ihre Arbeitnehmer zu erlangen.

Es gebe sowohl die Möglichkeit, Arbeitnehmer im Büro (durch den PC, den Server, das Telefon, durch eine Kamera oder Wanze, das Faxgerät oder den Kopierer), im Betrieb (durch Funkchips, durch eine Kamera oder Wanzen) oder unterwegs (durch das Handy, das Notebook oder den Dienstwagen) zu kontrollieren. Die technischen Einrichtungen würden dabei

immer ausgefeilter und würden die unterschiedlichsten Möglichkeiten zur Überwachung ermöglichen. *Wedde* hob dabei die folgenden technischen Varianten hervor:

a. Voice over IP (VoIP)

Die Einrichtung Voice over IP ermögliche das kostengünstige Telefonieren über das Internet. Standardtelefonanlagen würden daher immer häufiger durch internetbasierte Telefone ersetzt. Die Vermittlungsanlage sei dann nur noch ein Stück Software im betrieblichen Server. Dadurch werde die Kontrolle von Gesprächen erheblich erleichtert. Wer nämlich die Macht über den Vermittlungsrechner habe, könne aus technischer Sicht Gespräche speichern und unter Nutzung entsprechender Software auch auswerten. Der Benutzer des Telefons merke hiervon nichts.

Bei der sog. Fritz!-Anlage benötige man beispielsweise nur die Telefonnummer und die Kundennummer und könne das Gespräch dann mithören.

b. Spyware

Immer mehr Spionageprogramme - auch Spyware genannt - ermöglichen es laut *Wedde*, jeden PC (Nutzer) vollständig zu kontrollieren. Auch diese Programme könnten so eingestellt werden, dass die Kontrolle völlig unbemerkt bleibe.

So sei beispielsweise das Programm Cain & Abel in der Lage, gespeicherte Passwörter auszulesen und verschlüsselte Passwörter zu knacken. Ferner könnten VoIP-Gespräche abgehört sowie Routing-Prozesse analysiert werden. Seit Inkrafttreten des sog. Hackerparagrafen Ende Mai 2007 sei dieses Programm jedoch illegal.

c. RFID – Radio Frequency Identification

Mit Hilfe der Technologie RFID könne eine eindeutige und kontaktlose Identifizierung von Objekten jeglicher Art mit Hilfe elektromagnetischer Wellen erfolgen. Die Technologie könne mit Hilfe eines Transponders (Gehäuse, Antenne, Mikrochip) eingesetzt werden, so beispielsweise in Firmenausweisen und ermögliche es dann, umfassende Bewegungsprofile und -kontrollen durchzuführen.

d. Kontrolle per Navigationssystem (Navi) und Handy

Auch die Kontrolle per Navi und Handy ermögliche eine umfassende Kontrollmöglichkeit mobiler Arbeitnehmer.

So erläuterte *Wedde* weiter, dass sich die Daten eines Navis ganz einfach am Ende eines Arbeitstages auslesen und verwerten ließen. Die Auswertung der Daten eines Navis würden dem Arbeitgeber umfassende Informationen geben. So würden Navigationsgeräte die Fahrzeugdaten speichern, d. h. wann sich der Arbeitnehmer zu welcher Zeit an welchem Ort aufgehalten habe und damit auch einen Zugriff auf die Feststellung des Tempos und der genauen Ortung des Arbeitnehmers ermöglichen. Ferner lasse sich mittlerweile durch eine GMS-Ortung per Handy eine relativ genaue Ortung eines Arbeitnehmers vornehmen. Dafür benötige man neben einem Mobiltelefon nur noch eine spezielle Software und administrative Vorkehrungen.

Die GMS-Ortung per Handy biete dort neue Möglichkeiten, wo GPS-Systeme ihre physikalischen Grenzen erreichten, wie beispielsweise in Gebäuden.

Tatsächlich sei eine GMS-Ortung eines Arbeitnehmers kein Problem für Arbeitgeber. Praktisch jeder verfüge heute über die dafür notwendigen technischen Mittel (z. B. das Mobiltelefon) und die Geräte für spezielle Überwachungsmaßnahmen seien überall käuflich zu erwerben. Die Ortung sei auch möglich, ohne dass dies vom Überwachten bemerkt werde, so dass niemand vor Überwachungen sicher sein könne.

Im Ergebnis hielt *Wedde* fest, dass es für Arbeitgeber eine Fülle neuer technischer Möglichkeiten gebe, um ihre Beschäftigten zu beobachten und zu kontrollieren.

## 3. Bewertung der Situation aus arbeitsrechtlicher und datenschutzrechtlicher Sicht

Trotz der technischen Möglichkeiten und der zahlreichen „Vorfälle" der letzten Jahre sei es, so *Wedde,* bislang nur zu bescheidenen Veränderungen des Bundesdatenschutzgesetzes gekommen. Die Reaktion des Gesetzgebers auf die seit Jahren bestehenden oder absehbaren technischen Möglichkeiten sei als verhalten zu bewerten.

Auch die vom Gesetzgeber als „großer Wurf" angekündigte neue grundlegende Regelung zum „Beschäftigtendatenschutz" im BDSG weist laut *Wedde* umfassende Schwächen auf.

### a. Aktuelle Gesetzeslage

In der aktuellen Fassung des BDSG seien die folgenden allgemeinen Regelungen im Bereich des Beschäftigtendatenschutzes zu beachten:

§ 4 BDSG normiert den allgemeinen Grundsatz: „Es ist alles verboten, was nicht erlaubt ist", d. h. die Datenerhebung, -verarbeitung und -nutzung ist nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. § 3a BDSG regelt das Ziel, dass so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen sind. An die Einwilligung des Betroffenen sind gemäß § 4a BDSG hohe Anforderungen zu stellen.

Für den Beschäftigtendatenschutz gilt die Spezialregelung des § 32 BDSG. Von der Regelung sind neben Arbeitnehmern auch andere Beschäftigte umfasst.

*Wedde* ging sodann im Detail auf die Regelung des § 32 BDSG ein und erläuterte sie wie folgt:

- Gemäß § 32 Abs. 1 Satz 1 BDSG dürfen Arbeitgeber in laufenden Beschäftigungsverhältnissen nur solche Daten erheben, die für die Durchführung erforderlich sind. Der Begriff der Erforderlichkeit ist dabei mit Blick auf die Interessen der Beschäftigten nach Auffassung von *Wedde* eng auszulegen. Erforderlich ist eine Datenerhebung nach der Rechtsprechung nur dann, wenn der Arbeitgeber ein „berechtigtes, billigenswertes und schutzwürdiges Interesse" hat.

- Gemäß § 32 Abs. 1 Satz 2 BDSG dürfen Daten ausnahmsweise (unter engen Voraussetzungen) zur Aufdeckung von Straftaten erhoben, verarbeitet und genutzt werden.

- Gemäß § 32 Abs. 2 BDSG ist Abs. 1 auch auf die Führung von Akten (nicht automatisierte Dateien) anwendbar.

- Gemäß § 32 Abs. 3 BDSG bleiben Beteiligungsrechte von Betriebs- und Personalräten unberührt.

b. § 32 BDSG und die Rechtsprechung

*Wedde* erläuterte weiter, dass der Gesetzgeber in der Begründung zu § 32 BDSG ausdrücklich darauf verwiesen habe, dass diese Regelung den Stand der Rechtsprechung zum Beschäftigtendatenschutz wiedergibt. So haben sowohl das Bundesverfassungsgericht als auch das Bundesarbeitsgericht wegweisende Vorgaben in Bezug auf den Beschäftigtendatenschutz gemacht. Hierzu führte *Wedde* aus:

- 1983 hat das BVerfG das Recht auf informationelle Selbstbestimmung festgelegt und bestimmt, dass jedermann das Recht zusteht, über seine eigenen Daten selber zu verfügen.

- Mit einer Entscheidung aus dem Jahr 1991 hat das BVerfG bestimmt, dass Telefongespräche auch im Arbeitsverhältnis grundsätzlich vertraulich sind und heimliche und unbemerkte Abhörmaßnahmen verboten sind.

- Im Jahr 2008 äußerte sich das BVerfG zu Onlineuntersuchungen durch den Arbeitgeber. Danach sind heimliche Kontrollen mittels der Daten in IT-Systemen stets unzulässig, wenn nicht ein „schwerwiegender Grund“ vorliegt. Aber auch offene Kontrollen sind nicht zulässig, wenn Beschäftigte auf die Nutzung der IT-Systeme angewiesen sind, um ihre Arbeitsleistung zu erbringen oder wenn private oder persönliche Daten vorhanden sind, die zum Kernbereich des Persönlichkeitsrechts gehören. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) umfasst nach der Entscheidung des BVerfG das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

- Eine letzte wichtige Entscheidung in Bezug auf den Beschäftigtendatenschutz fällte das BVerfG im Jahr 2010. Dort nahm das BVerfG zur Unzulässigkeit von Vorratsdatenspeicherung Stellung.

- Aber auch das Bundesarbeitsgericht war in Bezug auf den Beschäftigtendatenschutz nicht untätig. 1997 entschied das BAG, dass das heimliche und unbemerkte Abhören von Telefongesprächen unzulässig ist.

- Mit der sog. Nikolausentscheidung vom 06.12.1983 hat das BAG beschlossen, dass ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG schon dann besteht, wenn

eine technische Einrichtung Verhaltens- und Leistungskontrollen auch nur ermöglicht. Auf einen Überwachungswillen kommt es nach der Auffassung des BAG nicht an.

- Im Jahr 2003/2004 hat das BAG entschieden, dass Beschäftigte vor heimlicher und ausufernder Videoüberwachung zu schützen sind. So ist der Arbeitgeber verpflichtet, im Falle des Bestehens von milderen Kontrollmöglichkeiten diese anstelle von permanenten Videokontrollen zu nutzen. So verlangt das Bundesarbeitsgericht, dass der Arbeitgeber auf technische Kontrollen verzichtet, wenn diese alternativ auch durch zusätzliches Personal durchgeführt werden können. In Fällen, in denen Kontrollen unverzichtbar sind, wie etwa im Wertbriefbereich eines Postverteilzentrums muss der Arbeitgeber die Kontrollen so gestalten, dass der Eingriff in Persönlichkeitsrechte so gering wie möglich ist. Dies kann beispielsweise umgesetzt werden, indem auf eine Aufzeichnung durch Kameras zugunsten einer Beobachtung der Bildschirme durch Personal verzichtet wird.

- Im Jahr 2008 hat das BAG Videoüberwachungen in bestimmten Fällen für zulässig erklärt, wenn sie als verhältnismäßig anzusehen sind.

c. Konsequenzen und Probleme

*Wedde* fasste sodann die Konsequenzen der Gesetzeslage unter Berücksichtigung der Rechtsprechung im Bezug auf Kontrollen aller Art im Arbeitsverhältnis zusammen. Danach seien

- heimliche und verdeckte Kontrollen im Arbeitsverhältnis immer unzulässig,

- offene Kontrollen nur zulässig, wenn sie objektiv notwendig seien und dem Arbeitgeber keine milderen Mittel zur Verfügung stünden,

- im Hinblick auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Eingriffe in den Kernbereich persönlicher Daten für den Arbeitgeber unzulässig.

Nicht gelöst seien jedoch bisher die folgenden Fragen:

- ob und in welchem Umfang dem Arbeitgeber Kontrollbefugnisse bei verbotener privater Nutzung durch den Beschäftigten zustehen,

- inwieweit es zulässig ist, Bewerber zu „googeln“,

- wie mit Arbeitnehmerdaten in Konzernstrukturen umzugehen ist,

- in welchem Umfang Videoüberwachungen zulässig sind,

- wie mit freiwilligen Einwilligungen etc. umzugehen ist.

d. Gesetzesnovelle 2011 und deren Bewertung

Weiter führte *Wedde* aus, dass der Gesetzgeber es sich zum Ziel gesetzt habe, alle offenen Fragen mit der Ergänzung des BDSG durch entsprechende Regelungen zum Beschäftigtendatenschutz zu beantworten. Durch die Novelle 2011 des BDSG sollte die Rechtssicherheit für Arbeitgeber und Beschäftigte erhöht werden. Dabei sollte ein ausgewogenes Verhältnis zwischen dem Interesse der Beschäftigten vor der unrechtmäßigen Erhebung und Verwendung ihrer Daten und dem Informationsinteresse des Arbeitgebers geschaffen werden.

Für die Erreichung dieser Ziele wollte der Gesetzgeber praxisgerechte Regelungen für Beschäftigte und Arbeitgeber schaffen, die klarstellen, dass nur erforderliche Daten erhoben, verarbeitet und genutzt werden dürfen.

Die Bewertung der Novelle durch *Wedde* fiel kritisch aus:
Positiv sei, dass der Gesetzgeber endlich ein umfassendes Regelwerk für den Beschäftigtendatenschutz schaffe und von der Rechtsprechung postulierte Vorgaben festgeschrieben würden. Ferner würden sinnvolle Vorgaben und Auswertungsbegrenzungen für neue technische Anwendungen in dem Gesetzesentwurf festgeschrieben, so z. B. zu biometrischen Verfahren in § 32f BDSG oder für Ortungssysteme in § 32g BDSG.

Der Gesetzesentwurf sei aber weder „übersichtlich“ noch „leicht verständlich“ und löse viele der bekannten und auch der aktuellen Probleme nicht. Die Beschäftigten würden durch die Novelle insbesondere nicht besser vor unzulässigen Erhebungen, Verarbeitungen oder Nutzungen ihrer Daten geschützt. Dies sei jedoch das eigentliche Ziel des „Beschäftigtendatenschutzes“ gewesen. Der Gesetzesentwurf räume Arbeitgebern weitgehende Erhebungs- und Verarbeitungsbefugnisse ein; so erlaube § 32 Abs. 6 BDSG-E die Erhebung von bestimmten Bewerberdaten aus dem Internet („Googeln“ wird erlaubt) und nach § 32a BDSG-E blieben ärztliche Untersuchungen im weiten Umfang zulässig. Ferner werde gemäß § 32i BDSG-E die inhaltliche Auswertung von dienstlichen E-Mail-Daten zulässig und eine neue Regelung, nach der die Datenerhebung ohne Kenntnis der Beschäftigten mit dem Ziel der Aufdeckung und Verhinderung von Straftaten und anderer Pflichtverletzungen im Arbeitsverhältnis zulässig werde, werde in § 32e ins BDSG eingefügt. Der Arbeitgeber werde buchstäblich zur Ermittlungsbehörde.

Im Ergebnis hielt *Wedde* fest, dass Beschäftigte durch die Gesetzesnovelle nicht besser geschützt würden als vorher und viele Praxisprobleme bestehen blieben. Zahlreiche rechtliche Auseinandersetzungen seien damit vorprogrammiert.

Dem Referat schloss sich eine lebhafte Diskussion über den neuen Gesetzesentwurf und insbesondere auch zur Zulässigkeit von Urin- und Bluttests an. Zum Abschluss dankten *Kallmann* und *Grauvogel* dem Referenten für den interessanten Vortrag und luden alle zum Ausklang der Veranstaltung in eine bremische Gaststätte ein.

Insa Lühmann

Richterin, Arbeitsgericht Bremen-Bremerhaven